IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Yohe

SERIAL NO.: 10/727291 GROUP: 2437

FILED: 12/03/2003 EXAMINER: Williams

Declaration – Rule 1.132 pursuant to 37 CFR 41.33

I, Thomas P. Yohe, hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I am the inventor in the above-identified application. I hereby state as follows:

1. This is a Declaration in response to the Office Action of 1/14/2009 wherein it has become apparent that the Examiner may not understand the terminology which is found in the original specification and which provides the basis for the amendments to the independent claims in the pending application.

2. The last two full paragraphs of the originally filed specification lend clarification as to the novelty and unobviousness of the instant invention. The text inserted in brackets is that which would be the readily apparent meaning for anyone skilled in the art when reading the remainder of the paragraph.

Because the SSL connection is terminated by SSLAC *[wherein SSLAC is the end point connection and this is not interpreted by one skilled in the art as terminating the connection or no data can be transmitted]*, SSLAC can process the data in unencrypted form allowing it to apply data compression and other optimization techniques to the data stream. This is done in such a way that the credentials of the SSLAS are presented to the web browser without having violated the SSL paradigm because the private key of the SSLAS was never transmitted to SSLAC.

The above described embodiment is set forth by way of example and is not for the purpose of limiting the present invention. It will be readily apparent to those skilled in the art that obvious modifications, derivations and variations can be made to the embodiments without departing from the scope of the invention. For example, SSLAS does not need to reside on the web server, but it is contemplated that SSLAS will be remotely located on another computer interacting with the web server computer; or where SSLAC is running on a different computer than browser and can whose services can be shared *concurrently* by multiple browsers. Accordingly, the claims appended hereto should be read in their full scope including any such modifications, derivations and variations.

3. The contention that concurrent SSL connections are not readily apparent to those skilled in the art is ill-founded. Indeed the instant invention sets forth providing a first SSL connection (see excerpt of page 6 and 7 below) and then forms a second SSL connection as indicated in the remaining two paragraphs as set forth above wherein data can be transferred in an optimized manner. There are two SSL connections otherwise the SSL connection under which the original connection is made would be lost and not permit the second SSL connection to exist. The excerpt is as follows:

The operation of the invention can be understood from steps shown in FIGS. 2A and 2B. SSL acceleration client software intercepts 200 new SSL request for a SSL secure connection from the web browser to a target web server. The SSL acceleration client software then initiates 202 a SSL handshake with the SSLAS operably associated with the target web server computer and to start SSL connection. The SSLAS then determines 204 which CA certificate is operably assocated with the target web server. As part of the SSL handshake between SSLAC and SSLAS, the SSLAS sends 206 this CA certificate to SSLAC along with a public key. At this point a secure SSL session is established between SSLAC and SSLAS and all subsequent data traffic between SSLAC and SSLAS flows over this secure connection. The SSLAC software sends 208 the copy of

the CA certificate to the web browser for validation 210. Web browser software sends 212 a list of available encryption algorithms (ciphers) back to target web server (i.e., server computer 102). SSLAC software intercepts this from the browser and sends 214 a chosen cipher to the browser software. The web browser software creates 216 a secret key, encrypts using chosen cipher and using the previously received public key and sends 218 the encrypted secret key to the target server, which is intercepted and sent 219 through the SSL acceleration client software to the SSLAS software. SSLAS software de-encrypts 220 the secret key using the private key operably associated with the target server. SSLAS software sends 222 decrypted secret key back to SSLAS software via the secure SSL connection, wherein a "handshake" is completed and secure communications between the client computer's web browser and SSLAS software and by using the secret key, data can be accelerated between the client computer 104 and the web server computer 102 employing acceleration software, such as compression software of the SSL acceleration client/server software.

4. The thrust of the difference by virtue of the instant invention is that by establishing a second SSL connection using the claimed invention, there can be optimization techniques applied to the data which is transferred over the second connection. This is not so with prior cited technologies which are merely subject to transmitting data using SSL connections using encryption techniques which inhibited the ability to use optimization techniques because, by design, encryption renders data unintelligible.

5. Thus, the instant claimed invention calls for a system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

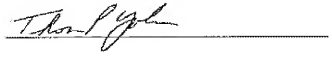
a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between said client and said web server, SSL acceleration client software operably associated with said client computer which communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second concurrent SSL connection between said client computer and said web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second concurrent SSL connection.

6. Nowhere in any of the cited references is there shown the above claimed invention which provide a unique structure and technique to enable optimization of data transfer while maintaining the SSL connection.

7. The instant invention is respectfully submitted to be patentably distinct over the art of record. Withdrawal of the rejection of claims 1-19 is respectfully requested.

Further, the declarant sayeth not.

Full name of inventor: Thomas P. Yohe



Inventor's signature Date 5/14/2009